Office of Protective Services

Counterintelligence / Counterterrorism Division

"Detect, Deter, and Neutralize"

NASA Counterintelligence Executive Brief

January 9, 2013

(SBU) Possible Foreign Intelligence Surveillance of a NASA Employee While on Official Overseas Travel and Useful Countermeasures

Prepared by the HQ CI/CT Office

(U) This CI Executive Brief was prepared by Special Agent Arthur Payton, NASA Headquarters Counterintelligence (CI)/Counterterrorism (CT) Office, (202) 358-4645. It is intended to increase awareness of the foreign intelligence threat to NASA employees while travelling overseas.

(U) EXECUTIVE SUMMARY:

- (SBU) In late 2012, during official overseas travel to a country that, historically, has engaged in aggressive intelligence collection against the United States and NASA, a senior NASA official experienced two suspicious/unusual events indicative of possible host nation intelligence service targeting.
    - (SBU) In the first instance, while looking for an item in an outer zipped pocket of a piece of luggage he left in his hotel room, the NASA employee discovered that his RSA token (which he had stored in that outer luggage pocket) had been detached from the lanyard that he normally used to carry the token. The employee found this highly unusual since the token was not easy to remove from the lanyard. For a general description of an RSA token, refer to Attachment 1.

    - (SBU) The second suspicious event occurred when the employee returned to his hotel room earlier that had originally been planned. As he approached his room he saw a housekeeper who appeared alarmed at his early return and ran up to him with the television remote from his room. The employee believed the housekeeper was almost in a panic that he would return to his room without the remote being there.
    - (SBU) The employee also mentioned observing multiple smoke detectors in hotel rooms he had previously stayed in during official travel to the same country. Similar reporting has been received from other NASA employees.
- **(SBU) NASA COUNTERTERRORISM PERSPECTIVE:**
    - (U) NASA is a world leader in the research, development, test, evaluation and fielding of leading-edge technologies. Our accomplishments awe and inspire the world. As such, it is also a target of foreign intelligence collection. Countries and companies can save substantial amounts of money stealing technology and can use that stolen information to challenge us culturally, militarily and economically.
    - (SBU) Though one may explain away the above events by saying the token was separated from its lanyard due to jostling during travel, that the housekeeper may have changed the batteries in the remote to ensure the guest had a properly working remote, and that the country visited is just security conscious when it comes to fire prevention, it's also likely that these events were related to host nation intelligence targeting of this and other NASA employees.

- (SBU) Though the RSA token is of no value to anyone without the accompanying PIN, it would be an interesting item to examine by someone searching the luggage of a NASA employee and discovering this unusual and interesting item. It would likely be photographed or otherwise inspected, time permitting.
- (SBU) Though the remote control may have been taken out of the room to change the batteries, it's also possible that it contained a digital recording device to capture room audio. It's also possible that biometric data was removed from it, for example, fingerprints.
- (SBU) Though it may give one a good sense of security seeing multiple smoke detectors in one's hotel room, one can go to the Internet and purchase legitimate-appearing smoke detectors containing hidden video recording devices.
- (SBU) The bottom line is: When traveling overseas, in particular for official business and where accommodations are arranged/provided by the host, assume your hotel room and work spaces contain clandestine audio and video surveillance devices.

- (SBU) NASA employees are advised to take into consideration that when traveling overseas, even to what would be considered "friendly" countries, there is always a chance that they and any electronic devices, documents, schematics, samples, etc., could be of interest to the host nation or other intelligence service.
  - (SBU) NASA employees traveling overseas, particularly for official travel (however, this service is offered for non-official travel as well) should contact their servicing NASA Counterintelligence/Counterterrorism Office for a pre-travel threat briefing. These briefings are mandatory for official travel to Designated Countries and Russia. A list of Designated Countries is at Attachment 2 of this report.
  - (SBU) In accordance with NASA Policy Directive 2540.1G, Personal Use of Government Office Equipment Including Information Technology, NASA employees shall only use loaner IT equipment during overseas travel (laptops, BlackBerries, iPhones, etc.). Employees should take only the information (reports, PowerPoint presentations, etc.) necessary for the trip (vs. one's life's work!). See Attachment 3 for the specific guidance.
  - (SBU) NASA employees should avoid using WIFI or other Internet connections overseas with NASA IT equipment to prevent the introduction of malware or other potential hostile intrusions.
  - (SBU) Beware of the Human Intelligence threat. Be careful of what you share with those you meet on overseas travel…to include your official foreign counterparts. This includes biographical data, the fact that you may work (previously, currently or planned) on other sensitive/classified projects, etc. Social cultivation of targeted employees is a common method to elicit information by foreign intelligence officers or their co-optees so don't let your guard down during social events, tours, meals, etc.
- (U) To report any foreign intelligence or terrorism threats/concerns, contact your Center or the HQ NASA Counterintelligence/Counterterrorism Office.

(U) DISTRIBUTION: All NASA.

ATTACHMENT 1

RSA Token Definition (from the Security Search website):

A security token (sometimes called an authentication token) is a small hardware device that the owner carries to authorize access to a network service. The device may be in the form of a smart card or may be embedded in a commonly used object such as a key fob. Security tokens provide an extra level of assurance through a method known as *two-factor authentication*: the user has a personal identification number (PIN), which authorizes them as the owner of that particular device; the device then displays a number which uniquely identifies the user to the service, allowing them to log in. The identification number for each user is changed frequently, usually every five minutes or so.

Unlike a password, a security token is a physical object. A key fob, for example, is practical and easy to carry, and thus, easy for the user to protect. Even if the key fob falls into the wrong hands, however, it can't be used to gain access because the PIN (which only the rightful user knows) is also needed.

Attachment 2, Designated Country Listing

	Code	Description	I	II	III	IV
					X	
	AF	Afghanistan				
	BA	Bahrain				X
	BO	Belarus			X	
	BT	Bhutan	X			
	BM	Burma (Now Myanmur)			X	
	CH	China, Peoples Republic			X	X
	CI	Cote D'Ivoire (Ivory Coast)			X	
	CG	Congo			X	
	CU	Cuba	X	X	X	
	CY	Cyprus			X	
	EG	Egypt				X
	ER	Eritrea			X	
**	FJ	Fiji			X	
	HA	Haiti			X	
	IR	Iran, Islamic	X	X	X	X
	IZ	Iraq			X	X
	IS	Israel				X
	JO	Jordan				X
	KN	Korea, North	X		X	X
	KU	Kuwait				X
	LE	Lebanon			X	X
	LI	Liberia			X	
	LY	Libyan Arab Jamahiriya			X	X
	MC	Macau (China)	X		X	X
	OM	Oman				X
	PK	Pakistan				X
	QA	Qatar				X
	RW	Rwanda			X	
	SA	Saudi Arabia				X
	SL	Saudi Leone			X	
	SO	Somalia			X	
	LK	Sri Lanka			X	
	SU	Sudan		X	X	
	SY	Syrian Arab Republic		X	X	X
	TW	Taiwan,	X			
	TC	United Arab Emirates				X
	VE	Venezuela			X	
	VM	Viet Nam			X	
	YM	Yemen			X	X
	ZI	Zimbabwe			X	

** - DDTC has published restrictive guidance regarding these entities, noted in the August 2010 ITAR Handbook notes, 22 CFR 126.1; or on the DDTC website.

***Key to Designated Status**

I. Countries with which the United States has no Diplomatic Relations
II. Countries determined by the Department of State to support Terrorism
III. Countries under Sanction or Embargo by the United States
IV. Countries of Missile Technology Concern (15 CFR 740 Appendix D:4, of the Export Administration Regulations, administered by the Bureau of Industry

Attachment 3

Excerpt from NPD 2540.1G

Personal Use of Government Office Equipment Including Information Technology

g. Removing Equipment from the Workplace

(1) Domestic Travel - When IT and/or computer equipment is taken out of the workplace (i.e., telework, offsite business meetings, conferences), it is the responsibility of the employee to ensure that the equipment remains in their custody, is handled and maintained properly, and is returned in good condition. In the event that the equipment is lost, stolen, or damaged, the employee shall notify the Center Chief Information Officer (CIO) as soon as possible after the occurrence of an incident.

(2) International Travel - The employee shall use only equipment officially approved for use outside of the U.S. for international business meetings, conferences, symposia, etc. The employee must ensure that the hardware remains in their possession while outside the U.S. Any loss, damage, or tampering shall be reported immediately/at the earliest opportunity to the Center CIO. Under no circumstances should Agency laptops or personal computers be used for official business on International trips unless written authorization is first obtained from the Center CIO.